Logica per l'informatica

Luca Tagliavini

February 25, 2022

0.1 Definizioni

Operazione associativa: $\forall x, y, z. \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Operazione commutativa: $\forall x, y. \quad x \cdot y = y \cdot x$
Rel eq indotta da una funzione: $a \sim fb = def = f(a) = f(b)$
Rel eq indotta da un sottogruppo: $a \sim Pb = def = (a + -b) \in P$
Immagine di una permutazione: $f : \mathbb{A} \longrightarrow \mathbb{B}$ si ha $Imm(f) = \{b \in \mathbb{B}\}$
NOTA: *applicare a b la struttura particolare degli elementi ritornati da f* in modo da poter ricavare (informalmente) una serie di condizioni per le quali un elemento appartiene a $\mathbb{B}$

Classe di equivalenza: $[x]_\sim = \{y \in A \mid x \sim y\}$
Quozientamento: $\circ_/$ di un insieme A si usa l'assioma di separazione dicendo $A_\sim = \{[x]_\sim \mid x \in A\}$

Kernel di una permutazione: $f : \mathbb{A} \longrightarrow \mathbb{B}$ si ha $Ker(f) = f^{-1}(e)$ dove e e' l'elemento neutro di $\mathbb{B}$
NOTA: per scegliere l'e corretto *ricordarsi cosa prende come argomento* f^{-1}
NOTA: espandendo poi questa definizione (sempre con l'assioma di separazione) si giunge a una serie di condizioni che definiscono gli elementi $\in Ker(f)$

Classi laterali: la scrittura $a\mathbb{B}$ o $\mathbb{B}a$ indicano le classi laterali di un insieme B rispettivamente da sinistra o da destra. Le classi sono formate utilizzando l'operazione dell'insieme $\mathbb{B}$ su ogni elemento $\in \mathbb{B}$ e con a.
Sottogruppo normale: Si dimostra in vari modi: o e' il sottogruppo di un gruppo (genitore) abeliano(la cui operazione e' commutativa), oppure si puo' provare che le classi lateriali di sinistra sono equivalenti alle classi lateriali di destra. Le suddette classi laterali andranno formate componendo il sottogruppo con tutti gli elementi del gruppo (genitore)

Permutazioni: cambiamento dell'ordine degli elementi all'interno di un insieme.
Definizioni possibili di permutazione:

- informalmente: una funzione che cambia l'ordine degli elementi

- formalmente: funzione biettiva $\mathbb{A} \longrightarrow \mathbb{A}$

0.2 How to

$(\mathbb{A}, \circ)$ semigruppo sse:

- $\circ$ chiusa rispetto a $\mathbb{A}$
- $\circ$ e' associativa

Si dimostra facendo $\forall a, b, c \in \mathbb{A}. \quad a \circ (b \circ c) = (a \circ b) \circ c$
Devo arrivare a far vedere che il risultao di $\circ$ ha una forma tale da appartenere ad $\mathbb{A}$

$(\mathbb{A}, \circ, n)$ monoide sse:

- n è l'elemento neutro di $\mathbb{A}$ e $\circ$

Si dimostra facendo $\forall a \in \mathbb{A}. \quad a \circ n = a$

$(\mathbb{A}, \circ, n, \circ^{-1})$ gruppo sse:

- $\circ^{-1}$ è la funzione inverso

Si dimostra facendo $\forall a \in \mathbb{A}. \quad a \circ a^{-1} = n$

Per dimostrare che un **gruppo è sottogruppo di un'altro gruppo** devo far vedere che le operazioni sono chiuse al sostegno del sottogruppo e che l'elemento neutro appartiene al sostegno del sottogruppo.

NOTA: in generale quando si espandono definizioni con l'assioma di separazione e' bene se si lavora su un insieme piccolo e ci sono facili risultati ca calcolare esporli, avvalendosi eventualmente dei punti di sospensione $(\ldots)$

f morfismo di $\mathbb{A}$ in $\mathbb{B}$: dove $(\mathbb{A}, \circ, 0, \cdot^{-1})$ e $(\mathbb{B}, \star, 00, \star^{-1})$

1. f deve essere t.c. $f : \mathbb{A} \longrightarrow \mathbb{B}$
2. $f(a \circ b) = f(a) \star f(b)$
3. $f(0) = 00$
4. $f(\circ^{-1}(a)) = \star^{-1}(f(a))$

0.3 Teoremi

0.3.1 Compattezza

Th: $\forall \Gamma, F$ se $\Gamma \models F$ allora esiste un $\Delta \subseteq \Gamma$, Δ finito t.c. $\Delta \models F$
Dim: Siano Γ, F t.c. $\Gamma \models F$. Per il teorema di completezza forte ho che $\Gamma \vdash F$. Esiste dunque un albero di deduzione naturale t.c. dimostra F e le cui foglie non scaricate formano un sottoinsieme finito Δ t.c. $\Delta \vdash F$. Per il teorema della correttezza si ha che $\Delta \models F$. qed

0.3.2 Completezza

Th: $\forall \Gamma, F. \quad \Gamma \models F \Rightarrow \Gamma \vdash F$

0.3.3 Correttezza

Th: $\forall \Gamma, F. \quad \Gamma \vdash F \Rightarrow \Gamma \models F$

0.3.4 Deduzione semantica

Th: $\forall \Gamma, F, G. \quad \Gamma \models (F \Rightarrow G) \iff \Gamma, F \models G$

0.3.5 Invarianza per sostituzione

Th: $\forall F, G_1, G_2$ formule, $\forall A. \quad G_1 \equiv G_2 \Rightarrow F[G_1/A] \equiv F[G_2/A]$

0.4 Definizioni

0.4.1 Soddisfacibile

Definizione: F soddisfacibile quando $\exists v.v \models F$
Con tabelle di verita': Una formula F si dice soddisfacibile se la sua tabella di verita' contiene almeno una riga nella quale la formula ha valore 1
Formula soddisfatta: F si dice soddisfatta in un mondo v ($v \models F$) sse $v(F) = 1$

0.4.2 Tautologia

Definizione: F tautologica quando $\forall v.v \models F$
Con tabelle di verita': Una formula F si dice tautologica se la sua tabella di verita' e' composta solamente da linee dove la formula ha valore 1

0.4.3 Insoddisfacibile

Definizione: F insoddisfacibile quando $\forall v.v \not\models F$ in alternativa $\nexists v.v \models F$
Con tabelle di verita': Una formula F si dice insoddisfacibile se la sua tabella di verita' e' composta solamente da linee dove la formula ha valore 0

0.4.4 Equivalenza Logica

Informale: $F \equiv G$ quando in ogni mondo F e G hanno la stessa denotazione, ovvero sono due connotazioni diverse per la stessa denotazione
Formale: $\forall F, G. \quad F \equiv G \iff (F \models G \land G \models F)$
Alternativa: $\forall v. [\![F]\!]^v = [\![G]\!]^v$

0.4.5 Conseguenza logica

Definizione: $\Gamma \models F$ quando $\forall v. (\forall G \in \Gamma. [\![G]\!]^v = 1) \Rightarrow [\![F]\!]^v = 1$
Definizione informale: $\Gamma \models F$ quando per tutti i mondi v si ha che tutte le ipotesi (filtri) in Γ sono vere (=1), allora anche F e' vera (=1).

0.4.6 Regola localmente corretta

Una regola si dice localmente corretta sse

$$\dfrac{\begin{array}{ccc}[\Delta_1] & & [\Delta_n] \\ \vdots & & \vdots \\ F_1 & \dots & F_n\end{array}}{G} \qquad (\Delta_1 \Rightarrow F_1, \dots, \Delta_n \Rightarrow F_n) \models G$$

0.4.7 Regola invertibile

Una regola si dice invertibile sse

$$\dfrac{F_1 \qquad \dots \qquad F_n}{G} \quad \forall i. G \models F_1, \dots, F_i$$

Ovviamente se ci sono ipotesi scaricate le si itroducono con un implica.
i.e. $G \models F_1, \dots, \Delta_4 \Rightarrow F_4, \dots, F_n$

0.5 Extra

0.5.1 Equivalenze notevoli

de mrogan:
$\neg(A \land B) \models \neg A \lor \neg B$ (in logica classica)
$\neg(A \lor B) \equiv \neg A \land \neg B$

de morgan (con quantificatori):
$\forall x. \neg P \equiv \neg \exists x. P$ (in logica classica)
$\exists x. \neg P \models \neg \forall x. P$ (in logica intuizionista, useless)
$\neg \exists x. P \equiv \forall x. \neg P$ (in entrambe)

de morgan (con quantificatori e operatori):
$(\forall x. P) \Rightarrow Q \equiv \exists x. (P \Rightarrow Q)$ (in logica classica)
$\exists x. (P \Rightarrow Q) \models (\forall x. P) \Rightarrow Q$ (in logica intuizionista, useless)
$(\exists x. P) \Rightarrow Q \equiv \forall x. (P \Rightarrow Q)$ (in entrambe)

0.5.2 Connettivi particolari

Esempi di connettivi con *nessuna* regola d'introduzione invertibili: $\vee$
Eesempi di connettivi con *solo* regole d'introduzione inveribili: $\Rightarrow, \neg, \wedge$

0.5.3 Cause di paradossi

1. uso meta-linguistico del linguaggio naturale
2. applicazione di un concetto meta-linguistico a se stesso
3. uso della negazione per concludere qualcosa e la sua negazione (i.e. $A \wedge \neg A$)